CLAIMS

What is claimed is:

1. A computer-implemented method for controling access to documents during a workflow, comprising:

upon entry of a base document into a workflow, creating a working copy of the base document;

selectively providing a user access to either the base document or the working copy of the base document depending upon the identity of a user; and

selectively providing access to perform operations on the working copy of the base document depending upon the identity of a user.

2. The method of claim 1, further comprising:

storing access control list data in relation to the base document, the access control list data defining access controls on performing operations of the working copy of the base document; and

storing security descriptor data in relation to the base document and the working copy of the base

document, the security descriptor data defining access controls on reading the base document and the working copy of the base document.

3. The method of claim 2, wherein the step of selectively providing access to perform operations on the working copy of the base document depending upon the identity of a user, further comprises:

determining using the access control list data stored in relation to the base document that a user has permission to perform an operation on the copy of the base document; and

allowing the user to perform the operation on the copy of the base document.

4. The method of claim 2, wherein the step of selectively providing access to perform operations on the working copy of the base document depending upon the identity of a user, further comprises:

determining using the access control list data stored in relation to the base document that a user does

not have permission to perform an operation on the copy of the base document; and

denying the user access to perform the operation on the copy of the base document.

5. The method of claim 2, wherein the access control list data comprises information identifying for each of a plurality of operations, the set of users that have permission to perform the operation, and said act of selectively providing access to perform operations on the working copy of the base document depending upon the identity of a user, further comprises:

referencing the information identifying for each of a plurality of operations, the set of users that have permission to perform the operation; and

if the user is in the set of users that have permission to perform the operation, providing access to the operation.

6. The method of claim 2, wherein the access control list data comprises information identifying for each of a plurality of operations, the set of users that have

permission to perform the operation, and said act of selectively providing access to perform operations on the working copy of the base document depending upon the identity of a user, further comprises:

referencing the information identifying for each of a plurality of operations, the set of users that have permission to perform the operation; and

if the user is not in the set of users that have permission to perform the operation, denying access to the operation.

7. The method of claim 5, wherein the set of users are defined in terms of the roles that have permission to perform the operation, and said act of referencing the information identifying for each of a plurality of operations, the set of users that have permission to perform the operation, further comprises:

resolving for the user the set of roles to which the user has been assigned; and

determining using the set of roles to which the user has been assigned and the set of users defined in terms of the roles that have permission to perform the

operation, whether the user has permission to perform the requested operation.

8. The method of claim 2, wherein the step of selectively providing a user access to either the base document or the working copy of the base document depending upon the identity of a user, further comprises:

determining using the security descriptor data stored in relation to the base document and the working copy document, that a user has permission to read the working copy of the base document; and

providing the user access to the working copy of the base document.

9. The method of claim 2, wherein the step of selectively providing a user access to either the base document or the working copy of the base document depending upon the identity of a user, further comprises:

determining using the security descriptor data stored in relation to the base document and the working copy document, that a user does not have permission to read the working copy of the base document; and

denying the user access to the base document.

10. The method of claim 2, wherein the security descriptor data comprises information identifying the set of users that have permission to read each of the base document and the working copy of the base document, and said act of selectively providing access to either the base document or the working copy of the base documents depending on the identity of the user, further comprises:

referencing the information identifying the set of users that have permission to read each of the base document and the working copy of the base document; and

if the user is in the set of users that have permission to read the working copy of the base document, providing access to the working copy of the base document.

11. The method of claim 10, wherein the set of users are defined in terms of the roles that have permission to read each of the base document and the working copy of the base document, and said act of referencing the information identifying the set of users that have permission to read

each of the base document and the working copy of the base document, further comprises:

resolving for the user the set of roles to which the user has been assigned; and

determining using the set of roles to which the user has been assigned and the set of user defined in terms of the roles that have permission to read each of the base document and the working copy of the base document, whether the user has permission to read the base document or the working copy of the base document.

12. A computer-readable media having stored thereon computer-executable instructions for performing the steps recited in claim 1.

13. A system for providing document isolation in a workflow environment, comprising:

a processor, wherein said processor is operable to execute instructions for performing the following acts:

maintaining for a base document undergoing a publishing workflow, a copy of the base document;

maintaining access control data in relation to the base document and the copy of the base document; and

determining based on the access control data, whether a user may access the base document or the copy of the base document.

14. The system of claim 13, wherein the access control data comprises security descriptor data identifying the set of users that have permission to read the base document and the copy of the base document.

15. The system of claim 14, wherein said processor is operable to execute instructions for performing the following further acts:

referencing the security descriptor data; and

determining that a user should be directed to the copy of the base document based on the security descriptor data.

16. The system of claim 15, wherein the security descriptor data identifies a set of roles corresponding to the set of users that have permission to read the base

document and the copy of the base document, and wherein said processor is operable to execute instructions for performing the further act of determining the set of roles that a user has been assigned.

17. The system of claim 13, wherein the access control data comprises access control list data identifying the set of users that have permission to perform operations on the copy of the base document.

18. The system of claim 17, wherein said processor is operable to execute instructions for performing the following further acts:

referencing the access control list data; and

determining that a user should be allowed to perform an operation on the copy of the base document based on the access control list data.

19. The system of claim 18, wherein the access control list data identifies a set of roles corresponding to the set of users that have permission to perform operations on the copy of the base document, and wherein

said processor is operable to execute instructions for performing the further act of determining the set of roles that a user has been assigned.

20. A method of updating access controls to reflect the addition of a new operation that may be performed on a copy of a base document, in a system wherein access to operations to be performed on a copy of the base document are controled using an access control list which identifies the operations that may be performed and the roles that a user must have to access those operations, comprising:

assigning a unique identifier to the new operation;

updating the access control list to include an entry for the unique identifier for the new operation;

updating the access control list to include an entry identifying the roles that have access to the new operation.